

# An analog of the Furstenberg-Katznelson-Weiss theorem on triangles in sets of positive density in finite field geometries

David Covert, Derrick Hart, Alex Iosevich and Ignacio Uriarte-Tuero

**ABSTRACT.** We prove that if the cardinality of a subset of the 2-dimensional vector space over a finite field with  $q$  elements is  $\geq \rho q^2$ , with  $\frac{1}{\sqrt{q}} \ll \rho \leq 1$ , then it contains an isometric copy of  $\geq c\rho q^3$  triangles.

## 1. Introduction

A classical result due to Furstenberg, Katznelson and Weiss ([4]; see also [1]) says that if  $E \subset \mathbb{R}^2$  has positive upper Lebesgue density, then for any  $\delta > 0$ , the  $\delta$ -neighborhood of  $E$  contains a congruent copy of a sufficiently large dilate of every three point configuration. An example due to Bourgain shows that if the three point configuration in question is an arithmetic progression, then taking a  $\delta$ -neighborhood is necessary and the result is not otherwise true. However, it seems reasonable to conjecture that if the three point configuration is non-degenerate in the sense that the three points do not lie on the same line, then a set of positive density contains a sufficiently large dilate of this configuration.

When the size of the point set is smaller than the dimension of ambient Euclidean space, taking a  $\delta$ -neighborhood is not necessary, as shown by Bourgain in [1]. He proves that if  $E \subset \mathbb{R}^d$  has positive upper density and  $\Delta$  is a  $k$ -simplex with  $k < d$ , then  $E$  contains a rotated and translated image of every large dilate of  $\Delta$ . The case  $k = d$  and  $k = d + 1$  remain open, however. See also, for example, [2], [3], [7], [11] and [13] on related problems and their connections with discrete analogs.

In the geometry of the integer lattice  $\mathbb{Z}^d$ , related problems have been recently investigated by Akos Magyar in [9] and [10]. In particular, he proves in [10] that if  $d > 2k + 4$  and  $E \subset \mathbb{Z}^d$  has positive upper density, then all large (depending on density of  $E$ ) dilates of a  $k$ -simplex in  $\mathbb{Z}^d$  can be embedded in  $E$ . Once again, serious difficulties arise when the size of the simplex is sufficiently large with respect to the ambient dimension.

The purpose of this paper is to investigate an analog of this question in finite field geometries. A step in this direction was taken by the second and third listed authors in [5]. They prove that if  $E \subset \mathbb{F}_q^d$ , the  $d$ -dimensional vector space over the finite field with  $q$  elements with  $|E| \geq Cq^{d\frac{k-1}{k} + \frac{k-1}{2}}$  and  $\Delta$  is a  $k$ -dimensional simplex, then there exists  $\tau \in \mathbb{F}_q^d$  and  $O \in SO_d(\mathbb{F}_q)$  such that  $\tau + O(\Delta) \subset E$ . The result is only non-trivial in the range  $d \geq \binom{k}{2}$  as larger simplexes are out of range of the methods used.

---

A. Iosevich was supported by the NSF Grant DMS04-56306.

The purpose of this paper is to address the case of triangles in two-dimensional vector spaces over finite fields. Given  $E \subset \mathbb{F}_q^2$ , define

$$T_3(E) = \{(x, y, z) \in E \times E \times E\} / \sim$$

with the equivalence relation  $\sim$  such that  $(x, y, z) \sim (x', y', z')$  if there exists  $\tau \in \mathbb{F}_q^2$  and  $O \in SO_2(\mathbb{F}_q)$ , the set of two-by-two orthogonal matrices over  $\mathbb{F}_q$  with determinant 1, such that

$$(x', y', z') = (O(x) + \tau, O(y) + \tau, O(z) + \tau).$$

Our main result is the following.

**THEOREM 1.1.** *Let  $E \subset \mathbb{F}_q^2$ , and suppose that*

$$|E| \geq \rho q^2$$

*for some  $\frac{C}{\sqrt{q}} \leq \rho \leq 1$  with a sufficiently large constant  $C > 0$ . Then there exists  $c > 0$  such that*

$$|T_3(E)| \geq c\rho q^3.$$

In other words, we show that if  $E$  has density  $\geq \rho$ , then the set of triangles determined by  $E$ , up to congruence, has density  $\geq c\rho$ , where  $\rho$  is allowed to depend on  $q$  within the parameters given above.

**REMARK 1.2.** Note that in contrast to the Furstenberg-Katznelson-Weiss result ([4]) we do not use dilations. This is natural because there is no order in  $\mathbb{F}_q$ , so a reasonable analog of proving a result for sufficiently large dilates of a three-point configuration in Euclidean space is proving it for all dilates in finite field geometries.

**REMARK 1.3.** Observe that the density condition  $|E| \geq \rho q^2$  immediately tells us that the numbers of three-tuples determined by  $E$ , up to congruence, is

$$\geq \frac{\rho^3 q^6}{q \cdot q^2} = \rho^3 q^3,$$

since the size of the translation group is  $q^2$  and the size of the rotation group is  $q$ . Thus our result can be viewed as shaving off two powers of  $\rho$  from this (trivial) estimate. It is conceivable that  $\rho q^3$  may be replaced by  $cq^3$ , for some  $0 < c < 1$ , or even  $(1 - o(1))q^3$ .

**1.1. Finite field analog of Bourgain's example.** The following variant of Bourgain's Euclidean construction (see [4]) shows that for general subsets of  $\mathbb{F}_q^2$  satisfying the density assumption  $|E| \geq \rho q^2$  for some  $\rho > 0$  it is not possible to recover isometric copies of all three point configurations.

Let  $A \subset \mathbb{F}_q^*$ , the multiplicative group of  $\mathbb{F}_q$ , such that  $|A| \geq \rho q$  for some  $\rho > 0$  and

$$2A + 2A - 4A \neq \mathbb{F}_q.$$

We shall give an (easy) construction of such a set at the end of the argument. Let

$$E = \bigcup_{t \in A} S_t,$$

where

$$S_t = \{x \in \mathbb{F}_q^2 : \|x\| = t\},$$

with

$$\|x\| = x_1^2 + x_2^2.$$

It is not difficult to check that  $|E| \geq \rho q^2$  using the classical fact that a circle in  $\mathbb{F}_q^2$  has  $q \pm 1$  points. See Lemma 3.2 below. Now consider a three-tuple

$$\left(x, y, \frac{x+y}{2}\right)$$

such that

$$||x - y|| \notin 2A + 2A - 4A.$$

We claim that such a three-tuple cannot be contained in  $E$ . We shall argue by contradiction. Indeed, the parallelogram law says that

$$2 \left\| \frac{x+y}{2} \right\|^2 + 2 \left\| \frac{x-y}{2} \right\|^2 = ||x||^2 + ||y||^2,$$

so

$$||x - y||^2 = 2||x||^2 + 2||y||^2 - 4 \left\| \frac{x+y}{2} \right\|^2,$$

which is an element of  $2A + 2A - 4A$ . By construction,  $||x - y|| \notin 2A + 2A - 4A$ , so we are done. It remains to show that the set  $A$  with the desired properties exists. Let  $q$  be a large prime number and denote the elements of the corresponding field  $\mathbb{F}_q$  by

$$\{0, 1, 2, \dots, q-1\}.$$

Let  $A$  consists of multiples of 8 that are less than or equal to  $q/32$ . This set is clearly of positive density and  $2A + 2A - 4A \neq \mathbb{F}_q$  since all of its elements are even as wrap-around is precluded from taking place by the condition that the largest element of  $A$  is  $\leq q/32$ .

REMARK 1.4. It is important to note that we do not *know* a single example of this type involving a non-degenerate triangle, one whose vertices do not lie on a line.

## 2. Proof of the main result (Theorem 1.1)

We prove Theorem 1.1 by reducing it to a statistically more precise statement about hinges. More precisely, we observe that it suffices to show that if  $|E| \geq \rho q^2$ , then

$$(2.1) \quad |\{(a, b, c) \in \mathbb{F}_q^3 : |T_{a,b,c}(E)| > 0\}| \geq c\rho q^3,$$

where

$$T_{a,b,c}(E) = \{(x, y, z) \in E \times E \times E : ||x - y|| = a, ||x - z|| = b, ||y - z|| = c\},$$

with

$$||x|| = x_1^2 + x_2^2.$$

This follows from the following simple lemma from [5], which we prove at the end of the paper for the sake of completeness.

LEMMA 2.1. *Let  $P$  be a (non-degenerate) simplex with vertices  $V_0, V_1, \dots, V_k$ , with  $V_j \in \mathbb{F}_q^d$ . Let  $P'$  be another (non-degenerate) simplex with vertices  $V'_0, V'_1, \dots, V'_k$ . Suppose that*

$$(2.2) \quad \|V_i - V_j\| = \|V'_i - V'_j\|$$

*for all  $i, j$ . Then there exists  $\tau \in \mathbb{F}_q^d$  and  $O \in SO_d(\mathbb{F}_q)$  such that  $\tau + O(P) = P'$ .*

The key estimate is the following result about hinges, which is interesting in its own right.

THEOREM 2.2. *Suppose that  $E \subset \mathbb{F}_q^2$  and let  $a, b \neq 0$ . Then*

$$|\{(x, y, z) \in E \times E \times E : \|x - y\| = a, \|x - z\| = b\}| = |E|^3 q^{-2} + O(q|E|).$$

We can use this result as follows. If  $|E| \gg q^{\frac{3}{2}}$ , then

$$|\{(x, y, z) \in E \times E \times E : \|x - y\| = a, \|x - z\| = b\}| = |E|^3 q^{-2} (1 + o(1)).$$

By the pigeon-hole principle, there exists  $x \in E$  such that

$$|\{(y, z) \in E \times E : \|x - y\| = a, \|x - z\| = b\}| \geq |E|^2 q^{-2}.$$

Suppose that the number of elements of  $SO_2(\mathbb{F}_q)$  that leave  $x$  fixed and keep  $(y, z)$  inside the pinned hinge is  $\leq \rho q$ . Then recalling our assumption that

$$|E| \geq \rho q^2,$$

we get that the number of distinct distances  $c$  from  $\{y \in E : \|x - y\| = a\}$  to  $\{z \in E : \|x - z\| = b\}$  is at least

$$|E|^2 q^{-2} \frac{1}{\rho q} \geq \frac{1}{2} \rho q,$$

and hence, since there are  $(q-1)$  possible choices for  $a$  and  $b$ , (2.1) follows.

If the number of elements of  $SO_2(\mathbb{F}_q)$  that leave  $x$  fixed and keep  $(y, z)$  inside the pinned hinge is  $> \rho q$ , then both the circle of radius  $a$ , centered at  $x$ , and the circle of radius  $b$ , centered at  $x$ , contain more than  $\rho q$  elements of  $E$ . The following simple lemma, whose proof is given at the end of this paper, shows that this implies that the number of distinct distances  $c$  from

$$\{y \in E : \|x - y\| = a\} \text{ to } \{z \in E : \|x - z\| = b\}$$

is  $\geq \frac{1}{4} \rho q$ , and thus (2.1) follows.

LEMMA 2.3. *Suppose that  $a, b, c \neq 0$ . Let  $w = (w_1, w_2) \in \{y \in \mathbb{F}_q^2 : \|x - y\| = a\}$ . Consider the set*

$$I = \{z \in \mathbb{F}_q^2 : \|x - z\| = b\} \cap \{u \in \mathbb{F}_q^2 : \|w - u\| = c\}.$$

*For at least  $\frac{q-3}{2}$  different values of  $c$ , we have that  $I \neq \emptyset$ .*

Thus the proof of Theorem 1.1 has been reduced to Theorem 2.2.

**2.1. Fourier analysis used in this paper.** Let  $\mathbb{F}_q^d$  be the  $d$ -dimensional vector space over the finite field  $\mathbb{F}_q$ . The Fourier transform of a function

$$f : \mathbb{F}_q^d \rightarrow \mathbb{C}$$

is given by

$$\widehat{f}(m) = q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x) \chi(-x \cdot m),$$

where  $\chi$  is an additive character on  $\mathbb{F}_q$ .

The orthogonality property of the Fourier Transform says that

$$q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot m) = 1$$

for  $m = (0, \dots, 0)$  and 0 otherwise. This property yields many of the standard properties of the Fourier Transform. We summarize the basic properties of the Fourier Transform used in this paper as follows.

LEMMA 2.4. *Let*

$$f, g : \mathbb{F}_q^d \rightarrow \mathbb{C}.$$

*Then*

$$\begin{aligned} \hat{f}(0, \dots, 0) &= q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x), \\ q^{-d} \sum_{x \in \mathbb{F}_q^d} f(x) \overline{g(x)} &= \sum_{m \in \mathbb{F}_q^d} \hat{f}(m) \overline{\hat{g}(m)}, \end{aligned}$$

*and*

$$f(x) = \sum_{m \in \mathbb{F}_q^d} \hat{f}(m) \chi(x \cdot m).$$

### 3. Proof of Theorem 2.2

Let

$$D_a = \{(x, y) \in E \times E : \|x - y\| = a\}$$

and identify  $D_a$  with its indicator function. We need the following result from [6], proved at the end of this paper for the sake of completeness.

THEOREM 3.1. *Let  $E \subset \mathbb{F}_q^d$  and suppose that  $t \neq 0$ . Then*

$$\sum_{x, y} D_t(x, y) = |E|^2 q^{-1} + O(q^{\frac{d-1}{2}} |E|).$$

Let

$$S_a = \{x \in \mathbb{F}_q^d : x_1^2 + \dots + x_d^2 = a\}$$

and identify  $S_a$  with its indicator function. Now setting  $d = 2$  and using Lemma 2.4 we see that

$$\begin{aligned} & |\{(x, y, z) \in E \times E \times E : \|x - y\| = a, \|x - z\| = b\}| \\ &= \sum_{x, y, z} D_a(x, y) E(z) S_b(x - z) \\ (3.1) \quad &= q^6 \sum_m \hat{D}_a(m, 0, 0) \hat{E}(m) \hat{S}_b(m). \end{aligned}$$

We need the following results about the Fourier transform of the sphere which we state in the  $d$ -dimensional context.

LEMMA 3.2. *Let  $d \geq 2$  and define  $S_b = \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = b\}$ . Suppose that  $b \neq 0$  and  $m \neq (0, \dots, 0)$ .*

$$(3.2) \quad |\widehat{S}_b(m)| \leq 2q^{-\frac{d+1}{2}}.$$

For any  $a \in \mathbb{F}_q^*$ ,

$$(3.3) \quad |S_a| = q^{d-1} + o(q^{d-1}).$$

We postpone the proof of the lemma until the end of the paper. In the meantime, we see that Lemma 2.4 implies that the expression in (3.1) equals

$$\begin{aligned} & |D_a| |E| |S_b| q^{-2} \\ & + q^6 \cdot \sum_{m \neq (0,0)} \widehat{D}_a(m, 0, 0) \widehat{E}(m) \widehat{S}_b(m) = I + R(a, b). \end{aligned}$$

In view of Lemma 3.2 and Theorem 3.1,

$$I = |E|^3 q^{-2} (1 + o(1)).$$

We have

$$R(a, b) = q^6 \sum_{m \neq (0,0)} \widehat{D}_a(m, 0, 0) \widehat{E}(m) \widehat{S}_b(m).$$

Using Lemma 3.2 once again and applying Cauchy-Schwartz followed by Lemma 2.4, we see that

$$\begin{aligned} |R(a, b)|^2 & \leq 4q^{-3} \cdot q^{12} \sum_m |\widehat{E}(m)|^2 \cdot \sum_m |\widehat{D}_a(m, 0, 0)|^2 \\ (3.4) \quad & = 4q^9 \cdot q^{-2} |E| \cdot \sum_m |\widehat{D}_a(m, 0, 0)|^2, \end{aligned}$$

and thus the matter is reduced to bounds for

$$\sum_m |\widehat{D}_a(m, 0, 0)|^2.$$

By definition,

$$\begin{aligned} \widehat{D}_a(m, 0, 0) & = q^{-4} \sum_{x, y} \chi(-x \cdot m) E(x) E(y) S_a(x - y) \\ & = q^{-2} \cdot q^{-2} \sum_x \chi(-x \cdot m) E(x) |E \cap S_a(x)|, \end{aligned}$$

where

$$S_a(x) = \{y \in \mathbb{F}_q^2 : \|x - y\| = a\}.$$

It follows from above and Lemma 2.4 that

$$\begin{aligned} \sum_m |\widehat{D}_a(m, 0, 0)|^2 & = q^{-4} \sum_m |\widehat{f}(m)|^2 \\ (3.5) \quad & = q^{-4} \cdot q^{-2} \sum_x |f(x)|^2, \end{aligned}$$

where

$$f(x) = E(x) |E \cap S_a(x)|,$$

and matters are reduced to the estimation of

$$\sum_x |f(x)|^2.$$

LEMMA 3.3. *With the notation above, if  $q$  is sufficiently large, then*

$$\sum_{x \in E} |E \cap S_a(x)|^2 \leq 8q|E|.$$

To prove the result, we write

$$\begin{aligned} |E \cap S_a(x)| &= \sum_y E(y) S_a(x - y) \\ &= |E| |S_a| q^{-2} + q^2 \sum_{m \neq (0,0)} \chi(x \cdot m) \widehat{E}(m) \widehat{S}_a(m) \\ &= A + B(x). \end{aligned}$$

It is easy to see that plugging in  $A$  leads to a better estimate than claimed. Now,

$$\begin{aligned} \sum_{x \in E} |B(x)|^2 &\leq \sum_{x \in \mathbb{F}_q^2} |B(x)|^2 \\ &= q^4 \sum_{m, m' \neq (0,0)} \widehat{E}(m) \overline{\widehat{E}(m')} \widehat{S}_a(m) \overline{\widehat{S}_a(m')} \sum_x \chi(x \cdot (m - m')) \\ &= q^6 \sum_{m \neq (0,0)} |\widehat{E}(m)|^2 |\widehat{S}_a(m)|^2, \end{aligned}$$

and by Lemma 3.2 this quantity is

$$\leq 4q^6 \cdot q^{-3} \sum_{m \neq (0,0)} |\widehat{E}(m)|^2,$$

which, by Lemma 2.4 is

$$\leq 4q|E|,$$

as claimed.

Plugging everything back into (3.5) and then (3.4), we see that

$$\begin{aligned} (3.6) \quad |R(a, b)|^2 &\leq 32q^9 \cdot q^{-2} \cdot |E| \cdot q^{-6} \cdot q|E| \\ &= 32q^2 |E|^2. \end{aligned}$$

Recall that

$$|\{(x, y, z) \in E \times E \times E : \|x - y\| = a, \|x - z\| = b\}| = I + R(a, b),$$

where

$$I = |E|^3 q^{-2} (1 + o(1))$$

and

$$|R(a, b)| \leq 8q|E|$$

for  $q$  sufficiently large by (3.6) above.

It follows that

$$|\{(x, y, z) \in E \times E \times E : \|x - y\| = a, \|x - z\| = b\}| = |E|^3 q^{-2} (1 + o(1))$$

if  $|E| > Cq^{\frac{3}{2}}$  with a sufficiently large constant  $C > 0$ , as claimed.

#### 4. Proof of Theorem 3.1

We have

$$\sum_{x,y} D_t(x,y) = \sum_{x,y} E(x)E(y)S_t(x-y).$$

Applying Fourier inversion to the sphere,

$$\begin{aligned} \sum_{x,y} D_t(x,y) &= \sum_{x,y} E(x)E(y) \sum_m \widehat{S}_t(m) \chi(m \cdot (x-y)) \\ &= q^{2d} \sum_m |\widehat{E}(m)|^2 \widehat{S}_t(m) \\ &= |E|^2 \cdot q^{-d} \cdot |S_t| + q^{2d} \sum_{m \neq (0,\dots,0)} |\widehat{E}(m)|^2 \widehat{S}_t(m) \\ &= M + R. \end{aligned}$$

By Lemma 3.2,

$$M = \frac{|E|^2}{q} + |E|^2 o(q^{-1}),$$

and using Lemma 3.2 once again, along with Lemma 2.4, we have

$$\begin{aligned} |R| &\leq 2q^{2d} \cdot q^{-\frac{d+1}{2}} \cdot \sum_m |\widehat{E}(m)|^2 \\ &= 2q^{\frac{d-1}{2}} \cdot |E|. \end{aligned}$$

This completes the proof.

#### 5. Proof of Lemma 3.2

For any  $l \in \mathbb{F}_q^d$ , we have

$$\begin{aligned} \widehat{S}_t(l) &= q^{-d} \sum_{x \in \mathbb{F}_q^d} q^{-1} \sum_{j \in \mathbb{F}_q} \chi(j(\|x\| - t)) \chi(-x \cdot l) \\ (5.1) \quad &= q^{-1} \delta(l) + q^{-d-1} \sum_{j \in \mathbb{F}_q^*} \chi(-jt) \sum_x \chi(j\|x\|) \chi(-x \cdot l), \end{aligned}$$

where the notation  $\delta(l) = 1$  if  $l = (0, \dots, 0)$  and  $\delta(l) = 0$  otherwise.

Now

$$\widehat{S}_t(l) = q^{-1} \delta(l) + Q^d q^{-\frac{d+2}{2}} \sum_{j \in \mathbb{F}_q^*} \chi\left(\frac{\|l\|}{4j} + jt\right) \eta^d(-j).$$

In the last line we have completed the square, changed  $j$  to  $-j$ , and used  $d$  times the Gauss sum equality (see e.g. [8])

$$(5.2) \quad \sum_{c \in \mathbb{F}_q} \chi(jc^2) = \eta(j) \sum_{c \in \mathbb{F}_q} \eta(c) \chi(c) = \eta(j) \sum_{c \in \mathbb{F}_q^*} \eta(c) \chi(c) = Q\sqrt{q} \eta(j),$$

where the constant  $Q$  equals  $\pm 1$  or  $\pm i$ , depending on  $q$ , and  $\eta$  is the quadratic multiplicative character (or the Legendre symbol) of  $\mathbb{F}_q^*$ .



The conclusion to the first and second parts of Lemma 3.2 now follows from standard Gauss sum estimates (see e.g. [8]) and the following classical estimate due to A. Weil ([12]).

THEOREM 5.1. *Let*

$$K(a) = \sum_{s \neq 0} \chi(as + s^{-1})\psi(s),$$

where  $\psi$  is a multiplicative character on  $\mathbb{F}_q^*$ . Then, if  $a \neq 0$ ,

$$|K(a)| \leq 2\sqrt{q}.$$

## 6. Proof of Lemma 2.1

Let  $\pi_r(x)$  denote the  $r$ th coordinate of  $x$ . Taking translations into account, we may assume that  $V_0 = (0, \dots, 0)$ . We may also assume that  $V_1, \dots, V_k$  are contained in  $\mathbb{F}_q^k$ . The condition (2.2) implies that

$$(6.1) \quad \sum_{r=1}^k \pi_r(V_i) \pi_r(V_j) = \sum_{r=1}^k \pi_r(V'_i) \pi_r(V'_j).$$

Let  $T$  be the linear transformation uniquely determined by the condition

$$T(V_i) = V'_i.$$

In order to prove that  $T$  is orthogonal, it suffices to show that

$$||Tx|| = ||x||$$

for any  $x \neq (0, \dots, 0)$ . We give this (standard) reduction below for the sake of reader's convenience.

Since  $V_j$ s form a basis, by assumption, we have

$$x = \sum_i t_i V_i,$$

so it suffices to show that

$$\begin{aligned} ||x|| &= \sum_r \sum_{i,j} t_i t_j \pi_r(V_i) \pi_r(V_j) \\ &= \sum_r \sum_{i,j} t_i t_j \pi_r(V'_i) \pi_r(V'_j) = ||Tx||, \end{aligned}$$

which follows immediately from (6.1).

Observe that we used the fact that orthogonality of  $T$ , the condition that  $T^t \cdot T = I$  is equivalent to the condition that  $||Tx|| = ||x||$ . To see this observe that to show that  $T^t \cdot T = I$  it suffices to show that  $T^t T x = x$  for all non-zero  $x$ . This, in turn, is equivalent to the statement that

$$\langle T^t T x, x \rangle = ||x||,$$

where

$$\langle x, y \rangle = \sum_{i=1}^k x_i y_i.$$

Now,

$$\langle T^t T x, x \rangle = \langle T x, T x \rangle$$

by definition of the transpose, so the stated equivalence is established. This completes the proof of Lemma 2.1.

### 7. Proof of Lemma 2.3

After a translation, we may assume without loss of generality that  $x = (0, 0)$ . We are looking for solutions  $(s, t)$  to the system of equations

$$(7.1) \quad \begin{cases} (s - w_1)^2 + (t - w_2)^2 = c \\ s^2 + t^2 = b \end{cases}$$

with the assumption that  $w_1^2 + w_2^2 = a$ . Then (7.1) is equivalent to

$$(7.2) \quad \begin{cases} w_1 \cdot s + w_2 \cdot t = \frac{a+b-c}{2} \\ s^2 + t^2 = b \end{cases}$$

Now  $w_1$  and  $w_2$  cannot be simultaneously zero since  $a \neq 0$ . If  $w_1 \neq 0$ , from the first equation in (7.2) we get that

$$(7.3) \quad s = \frac{1}{w_1} \left\{ \frac{a+b-c}{2} - w_2 \cdot t \right\},$$

which substituted into the second equation in (7.2) gives

$$(7.4) \quad \left\{ \left( \frac{w_2}{w_1} \right)^2 + 1 \right\} t^2 - \left\{ \frac{a+b-c}{w_1} \frac{w_2}{w_1} \right\} t + \left( \frac{a+b-c}{2w_1} \right)^2 - b = 0.$$

(If  $w_1 = 0$  so that  $w_2 \neq 0$ , the resulting equation is the same as (7.4) but interchanging the roles of  $w_1$  and  $w_2$  among themselves and the roles of  $s$  and  $t$  among themselves.)

However, notice now that the condition  $w_2 = \pm i w_1$  is incompatible with the hypothesis that  $w_1^2 + w_2^2 = a \neq 0$ . Consequently,  $\left( \frac{w_2}{w_1} \right)^2 \neq -1$ , and hence the equation (7.4) has at most 2 solutions. We still have to prove that the equation (7.4) has indeed a solution under our hypotheses. The discriminant of equation (7.4) is

$$(7.5) \quad \begin{aligned} \Delta &= \left\{ \frac{a+b-c}{w_1} \frac{w_2}{w_1} \right\}^2 - 4 \left\{ \left( \frac{w_2}{w_1} \right)^2 + 1 \right\} \left[ \left( \frac{a+b-c}{2w_1} \right)^2 - b \right] = \frac{4b[w_1^2 + w_2^2] - (a+b-c)^2}{w_1^2} = \\ &= \frac{4ab - (a+b-c)^2}{w_1^2}. \end{aligned}$$

Hence equation (7.4) has a solution precisely when there exists a  $k \in \mathbb{F}_q$  such that

$$(7.6) \quad 4ab - (a+b-c)^2 = k^2,$$

which happens precisely when  $c$  is of the form

$$(7.7) \quad c = a + b \pm \sqrt{4ab - k^2},$$

i.e. whenever there exists a  $\tau \in \mathbb{F}_q$  such that

$$(7.8) \quad k^2 + \tau^2 = 4ab.$$

We now repeat, for the convenience of the reader, the well-known argument that every element of  $\mathbb{F}_q$  is a sum of 2 squares. Namely, by (5.2), and recalling that  $\eta^2(t) = 1$  and that  $\sum_{t \in \mathbb{F}_q} \chi(-4abt) = 0$  if  $t \neq 0$ , and that  $Q = \pm 1$  or  $\pm i$  depending on  $q$ ,

$$\begin{aligned}
 |\{(k, \tau) : k^2 + \tau^2 = 4ab\}| &= \frac{1}{q} \sum_{t \in \mathbb{F}_q} \sum_{k, \tau \in \mathbb{F}_q} \chi(t(k^2 + \tau^2 - 4ab)) = \\
 &= q + \frac{1}{q} \sum_{t \neq 0} \sum_{k, \tau \in \mathbb{F}_q} \chi(t(k^2 + \tau^2 - 4ab)) = \\
 (7.9) \qquad &= q + \frac{1}{q} \sum_{t \neq 0} \chi(-4abt) Q^2 q \eta^2(t) = q - Q^2 .
 \end{aligned}$$

Hence equation (7.4) has a solution for at least  $\frac{q+1}{2}$  different values of  $c$ , since by (7.7) and (7.8) each value of  $c$  for which equation (7.4) has a solution corresponds precisely to one value of  $\tau$ , and each value of  $\tau$  is accounted for at most twice in (7.9) since for each such value of  $\tau$ , there are at most 2 values of  $k$  satisfying (7.8).

Since it is conceivable (depending on the value of  $q$ ) that  $c = 0$  yields a solution to (7.1), accounting for that possibility, we can assert that (7.1) has a solution for at least  $\frac{q-3}{2}$  different values of  $c \neq 0$ .

## References

- [1] J. Bourgain, *A Szemerdi type theorem for sets of positive density*, Israel J. Math. **54** (1986), no. 3, 307-331. [1](#)
- [2] V. Bergelson, *Ergodic Ramsey theory an update*, Ergodic Theory of  $\mathbb{Z}^d$ -Actions (Warwick, 1993–1994) (M. Pollicott and K. Schmidt, eds.), London Math. Soc. Lecture Note Ser., **228**, Cambridge Univ. Press, Cambridge, (1996). [1](#)
- [3] H. Furstenberg, *Recurrence in ergodic theory and combinatorial number theory*, M. B. Porter Lectures, Princeton Univ. Press, Princeton, NJ, (1981). [1](#)
- [4] H. Furstenberg, Y. Katznelson, and B. Weiss, *Ergodic theory and configurations in sets of positive density* Mathematics of Ramsey theory, 184-198, Algorithms Combin., 5, Springer, Berlin, (1990). [1](#), [2](#)
- [5] D. Hart and A. Iosevich, *Ubiquity of simplices in subsets of vector spaces over finite fields*, Analysis Mathematica, **34**, (2007). [1](#), [3](#)
- [6] A. Iosevich and M. Rudnev, *Erdős distance problem in vector spaces over finite fields*. Trans. Amer. Math. Soc. (2007). [5](#)
- [7] B. Kra, *Ergodic methods in additive combinatorics*, Centre de Recherches Mathematiques Proceedings and Lecture Notes (2007). [1](#)
- [8] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, (1997). [8](#), [9](#)
- [9] A. Magyar, *On distance sets of large sets of integers points*, Israel Math J. (to appear) (2006). [1](#)
- [10] A. Magyar, *k-point configurations in sets of positive density of  $\mathbb{Z}^n$* , Duke Math J. (to appear), (2007). [1](#)
- [11] T. Tao and V. Vu. *Additive Combinatorics*. Cambridge University Press, 2006. [1](#)
- [12] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948) 204-207. [9](#)
- [13] T. Ziegler, *An application of ergodic theory to a problem in geometric Ramsey theory*, Israel Journal of Math. **114** (1999) 271-288. [1](#)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MISSOURI, COLUMBIA, MO 65211-4100

*E-mail address:* `covert@math.missouri.edu`

*E-mail address:* `hart@math.missouri.edu`

*E-mail address:* `iosevich@math.missouri.edu`

*E-mail address:* `ignacio@math.missouri.edu`